Seminar

*Software Engineering für verteilte Systeme*

Sommersemester 2024

# Grafana: Sicherheitsaspekte in verteilten Systemen - Herausforderungen und Maßnahmen

-

Matrikelnummer: -

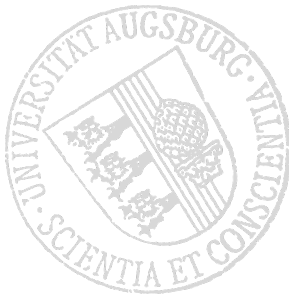
–

Betreuer: Marco Wölfel

Softwaremethodik für verteilte Systeme (Prof. Bauer)

Universität Augsburg

**Zusammenfassung** Diese Arbeit untersucht die Sicherheitsaspekte des Datenvisualisierung-Tools Grafana. Der Schwerpunkt liegt auf den Herausforderungen und Maßnahmen, die für die Absicherung von Grafana in verteilten Systemen notwendig sind. Es wird analysiert, welche Sicherheitsmaßnahmen in der Open-Source-Version von Grafana vorhanden sind und welche zusätzlichen Funktionen in den kommerziellen Varianten Grafana Cloud und Grafana Enterprise zur Verfügung stehen. Ziel ist es zu bewerten, ob die Funktionen für einen Einsatz im Kontext von verteilten Systemen ausreichende Sicherheit bieten.



# Inhaltsverzeichnis

# 1 Grafana Überblick

Grafana ist ein *Open-Source*-Tool für Datenvisualisierung und Monitoring, das besonders in der *IT-Überwachung* und *DevOps* eingesetzt wird. Es wurde erstmals 2014 veröffentlicht und hat sich seitdem zu einer der führenden Lösungen im Bereich der Datenvisualisierung entwickelt. Zu den Hauptmerkmalen von Grafana gehören anpassbare Dashboards, Unterstützung für zahlreiche Datenquellen und Alert-Funktionen. Grafana unterstützt eine Vielzahl von Datenquellen wie *Prometheus*, *InfluxDB*, *Elasticsearch*, *MySQL*, *PostgreSQL* und viele andere. Die Integration verschiedener Datenquellen ermöglicht es Nutzern, Daten aus verschiedenen Systemen und Anwendungen in einem einzigen Dashboard zusammenzuführen. Deswegen ist Grafana auch insbesondere für verteilte Systeme interessant, da Daten aus verschiedenen Systemen eingebunden werden können. Ein Vorteil von Grafana ist die benutzerfreundliche Oberfläche, die es ermöglicht, komplexe Datenvisualisierungen anhand von Tabellen, Graphen, Balkendiagrammen, Heatmaps etc. zu erstellen und zu verwalten. In Abbildung 1 ist ein Screenshot von Grafana dargestellt. Man kann darin die Visualisierung von verschiedensten Graphen entnehmen. Durch die Erstellung von Alerts und Benachrichtigungen kann der Nutzer auf kritische Ereignisse oder Abweichungen in den Daten hingewiesen werden. Des Weiteren bietet Grafana eine Vielzahl von Integrationen und Erweiterungen, um die Funktionalität und Anpassungsfähigkeit der Plattform zu erweitern. Typische Einsatzszenarien von Grafana umfassen *System-* und *Netzwerküberwachung*, *Performance-Analysen*, *Log-Management*, *Business Intelligence* und *IoT-Überwachung*. [1]
Security ist ein wichtiges Problem im Umgang mit Daten. Diese Arbeit soll einen Überblick über die Sicherheitsmaßnahmen von Grafana bieten und erklären, warum diese Maßnahmen wichtig sind, um Grafana möglichst abzusichern. Außerdem wird evaluiert, ob die Sicherheitsmaßnahmen im Kontext von verteilten Systemen ausreichend sind.


Abbildung 1: Ein Screenshot von Grafana, der verschiedene Visualisierungen darstellt [2].

# 2 Relevanz von Security

Das *CIA Triad* bildet die Basis für die Entwicklung von sicheren Informationssystemen. Es umfasst die drei essenziellen Prinzipien: *Confidentiality* (Vertraulichkeit), *Integrity* (Integrität) und *Availability* (Verfügbarkeit). *Confidentiality* stellt sicher, dass Daten nur von befugten Personen eingesehen werden können. *Integrity* gewährleistet die Richtigkeit und Unveränderlichkeit der Daten. *Availability* sorgt dafür, dass Daten jederzeit für befugte Benutzer zugänglich sind. [3]
Die *CIA Triad* wird durch Standards wie ISO/IEC 27001 erweitert, welcher das Management von Informationssicherheit beschreibt. Zusätzliche Prinzipien umfassen *Non-repudiation* (Nichtabstreitbarkeit), bei dem Entitäten ihre Aktionen nicht abstreiten können, *Authenticity* (Echtheit), die die Echtheit einer Entität sicherstellt, und *Accountability* (Verantwortlichkeit), bei der Aktionen wie Login und Datenveränderungen aufgezeichnet werden. [4]

## 2.1 Relevanz in verteilten Systemen

Die Datensicherheit ist in Grafana von besonderer Bedeutung, da der Zugriff auf eine große Menge sensibler Daten möglich ist. Dies ist besonders bei verteilten Systemen wichtig, da hier mehr Systeme betroffen sind. Wenn viele Datenquellen aus unterschiedlichen Systemen eingebunden sind, ist Grafana ein *Single Point of Failure* für Angreifer. Erlangt dieser Zugriff, ist eine große Datenmenge gefährdet, was gegen die *Confidentiality* verstößt. Die *Integrity* der Daten und Grafana-Alerts kann ebenfalls bedroht sein, wenn Änderungen am System vorgenommen werden. Viele Datenquellen erhöhen zudem die Komplexität, die Verwaltung und Übersicht werden schwieriger, was zu einem Verlust der *Integrity* führen kann, wenn die Berechtigungen nicht richtig verwaltet werden.
Unterschiedliche Zuständigkeiten für Datenquellen können ebenfalls ein Problem darstellen. Beispielsweise sollten Daten für *Key Performance Indicators* nur für den CEO zugänglich sein, während Produktionsdaten für einen Produktionsmitarbeiter zugänglich sein müssen. Dies betrifft die *Confidentiality*, da Mitarbeiter nicht auf Daten zugreifen sollten, die nicht für sie bestimmt sind.
Szenarien, die in Grafana zu einem Verlust der *CIA* führen können, sind vielfältig. Ein Serverabsturz könnte den Verlust von Daten zur Folge haben, wodurch Mitarbeiter nicht mehr auf ihre Dashboards zugreifen können, was die *Availability* verletzt. Ebenso kann eine *DDOS-Attacke* die Zugänglichkeit der Grafana-Instanz beeinträchtigen, was ebenfalls gegen die *Availability* verstößt. Ein weiteres Szenario könnte sein, dass ein Mitarbeiter Daten stiehlt, auf die er eigentlich keinen Zugriff haben sollte, das somit einen Verstoß gegen *Confidentiality* darstellt. Dies veranschaulicht, dass es viele Sicherheitsrisiken gibt, die mit entsprechenden Maßnahmen abschwächt werden müssen. Die Risiken mit verteilten Systemen sind sehr ähnlich wie bei herkömmlichen Datenquellen in Grafana. Die Auswirkungen sind jedoch häufig schlimmer, da die Zahl der betroffenen Systeme und Datenquellen meist viel größer ist.

## 2.2 Angriffe und Risiken

Man unterscheidet vor allem zwischen zwei verschiedenen Angriffspunkten. *Interne Threats* umfassen Mitarbeiter, die absichtlich oder unbeabsichtigt Schaden anrichten. Mitarbeiter mit böswilligen Absichten oder solche, die durch falsche Konfigurationen unbeabsichtigte Schäden verursachen, stellen ein erhebliches Risiko dar. Zum anderen existieren *Externe Threats*, wie Cyberkriminelle, Hacker, Hacktivists und Nation State Actors. Sicherheitslücken, wie die in der CVE-Datenbank dokumentierten Schwachstellen für Grafana [5], zeigen, dass solche Lücken existieren und ausgenutzt werden können.

# 3 Data Security in Grafana

Im Folgenden wird beschrieben, welche Sicherheitsfunktionen Grafana anbietet, um die Sicherheit der Daten zu gewährleisten.

## 3.1 Identity & Access Management (IAM)

*Identity & Access Management* (IAM) bezeichnet Systeme und Prozesse, die zur Verwaltung digitaler Identitäten und der Zugriffskontrolle auf Ressourcen innerhalb eines Unternehmens eingesetzt werden. IAM umfasst die Authentifizierung und Autorisierung von Benutzern, um sicherzustellen, dass nur berechtigte Personen Zugang zu bestimmten Systemen haben.
IAM betrifft alle drei Prinzipien der *CIA Triad*:
**Vertraulichkeit**: Wenn Authentifizierungs- und Autorisierungsmechanismen nicht ordnungsgemäß implementiert sind, können nicht autorisierte Benutzer Zugriff auf sensible Daten erhalten und deren Vertraulichkeit gefährden.
**Integrität**: Unzureichende Kontrollen bei der Authentifizierung und Autorisierung können zu unbefugten Änderungen an Dashboards oder Datenquellen führen und die Integrität der Informationen beeinträchtigen.
**Verfügbarkeit**: Eine unzureichende IAM kann die Verfügbarkeit der Grafana-Plattform und der bereitgestellten Daten beeinträchtigen, wenn Dritte Zugriff zu Admin-Accounts erhalten.

### 3.1.1 Authentication & Authorization

Grafana bietet verschiedene Authentifizierungsmethoden, um einen sicheren Zugriff auf die Plattform zu gewährleisten. Dazu gehören die Authentifizierung über Benutzername und Passwort, *SAML*, *OAuth* und mehr. [6]
Eine wichtige Komponente des IAM in Grafana ist die rollenbasierte Zugriffskontrolle (*RBAC*). Sie ermöglicht es Administratoren, Rollen zu definieren und Benutzern oder Gruppen basierend auf ihren Aufgaben und Zugriffsanforderungen Berechtigungen zuzuweisen. *RBAC* erlaubt eine Kontrolle darüber, was Benutzer innerhalb von Grafana tun können, z.B. das Erstellen von Dashboards, das Verwalten von Datenquellen oder der Zugriff auf bestimmte Funktionen. [7]

### 3.1.2 Dashboard & Folder Permissions

Grafana ermöglicht es Administratoren, Berechtigungen für Dashboards und Ordner festzulegen, um sicherzustellen, dass nur autorisierte Benutzer sie anzeigen oder bearbeiten können. Berechtigungen können auf Benutzerebene oder für Benutzergruppen gewährt werden, um die Zugriffskontrolle für mehrere Benutzer zu vereinfachen. Administratoren können Lese- oder Bearbeitungszugriff für bestimmte Benutzer oder Gruppen festlegen, abhängig von ihren Rollen und Aufgaben. Gemeinsam genutzte Dashboards können eigene Berechtigungen haben, sodass Benutzer kontrollieren können, wer darauf zugreifen und sie bearbeiten kann. [8]

### 3.1.3 Datasource Permissions

Grafana bietet eine Kontrolle über den Zugriff auf Datenquellen, um sicherzustellen, dass nur autorisierte Benutzer auf bestimmte Datenquellen zugreifen können. Administratoren können Berechtigungen für jede Datenquelle konfigurieren und festlegen, welche Benutzer oder Gruppen auf die Daten zugreifen und mit ihnen interagieren können. Dies hilft dabei, sensible Datenquellen zu schützen und sicherzustellen, dass nur autorisierte Personen die Daten anzeigen oder bearbeiten können. [9]

## 3.2 Datenbank Verschlüsselung

Grafana speichert in einer Datenbank *Secrets*, die zur Abfrage von Datenquellen, zum Versenden von Alert-Benachrichtigungen und zur Ausführung weiterer Funktionen in Grafana verwendet werden. Die Verschlüsselung der Datenbank ist entscheidend, um unbefugten Zugriff auf vertrauliche Informationen zu verhindern und somit die Vertraulichkeit (*Confidentiality*) zu gewährleisten. Für die Integrität (*Integrity*) der Datenquellen ist dies ebenfalls wichtig. Die *Secrets* werden durch AES mit einem in Grafana konfigurierten Schlüssel verschlüsselt. Dieser sollte regelmäßig durch einen Administrator rotiert werden, und besonders nach der initialen Konfiguration sollte der Default-Schlüssel ausgetauscht werden. Alternativ kann auch ein externes *Key Management System* (KMS) eingebunden werden, um eine erhöhte Sicherheit zu erhalten. Grafana unterstützt verschiedene Anbieter wie AWS KMS, Azure Key Vault, Google Cloud KMS und Hashicorp Vault. Dadurch können die *Secrets* in der Grafana-Datenbank mit einem Schlüssel verschlüsselt werden, der im zentralisierten Key-Store eines dieser Anbieter gespeichert ist. [10]

## 3.3 Auditing

Auditing in Grafana bezieht sich auf den Prozess der Überwachung und Aufzeichnung von Aktivitäten, die in Grafana stattfinden. Dies ermöglicht es Administratoren, die Aktivitäten der Benutzer zu überwachen, um Sicherheitsverletzungen zu erkennen, Compliance-Anforderungen zu erfüllen und potenzielle Bedrohungen zu identifizieren. Auditing wird vor allem eingesetzt, um interne Bedrohungen durch bereits autorisierte Nutzer zu verhindern. Zusätzlich hilft es, das Ausnutzen von Nutzerrechten eines kompromittierten

Accounts zu erkennen. Dadurch können die Prinzipien *Non-repudiation* (Nichtabstreitbarkeit) und *Accountability* (Verantwortlichkeit) sichergestellt werden. Um dies zu erreichen, zeichnet Grafana verschiedene Benutzeraktionen auf, wie z.B. Anmeldungen, Änderungen an Dashboards oder Datenquellen, Erstellung oder Löschen von Benutzern, Zugriff auf bestimmte Ressourcen usw. Die aufgezeichneten Aktivitäten werden in Audit-Logs gespeichert, die Informationen wie Zeitstempel, Benutzernamen, durchgeführte Aktion und betroffene Ressource enthalten und im JSON-Format abgespeichert werden. Um die Log-Daten zu visualisieren und zu analysieren, können diese in Grafana als Datenquelle eingebunden werden. Mit benutzerdefinierten Alerts können Benachrichtigungen verschickt werden, wenn beispielsweise Nutzeraktionen ungewöhnlich oft auftreten. Alternativ können die Audit-Log-Daten auch zu Grafana Loki geschickt werden, einem speziellen Log-Aggregationssystem von Grafana. [11]

## 3.4 Weitere Sicherheitsmaßnahmen

Grafana bietet weitere Sicherheitsmaßnahmen an, die konfiguriert werden können. Der *GitHub Secret Scanning Service* kann in Grafana verwendet werden, um versehentlich veröffentlichte Tokens automatisch zu sperren [12]. Des Weiteren kann Request Security konfiguriert werden, um die Anfragen an den Grafana Server anhand der *IP*, *deny* oder *allow list* zu blockieren bzw. zu limitieren [13].
Darüber hinaus ist es wichtig, regelmäßige Backups der Konfiguration und Datenbank durchzuführen, um im Falle eines Datenverlusts eine Wiederherstellung zu ermöglichen [14]. Regelmäßige Aktualisierungen von Grafana sollten ebenfalls durchgeführt werden, um von den neuesten Sicherheitspatches und -verbesserungen zu profitieren [15].
Grafana bietet verschiedene Sicherheitskonfigurationen, die zur Verbesserung der Sicherheit konfiguriert werden können. Dazu gehören die Verwendung von *HTTPS* für die sichere Übertragung von Daten, die Nutzung von sicheren Cookies, um bestimmte Angriffe zu verhindern, und die Implementierung von *Security-Headern*, wie einer *Content Security Policy* [16].

# 4 Security-Funktionen Evaluation

Es ist wichtig zu erwähnen, dass *Grafana* nicht alle Sicherheitsfunktionen in der kostenlosen Open-Source-Lizenz anbietet. Um eine höhere Sicherheit zu erreichen, muss der Nutzer auf *Grafana Cloud* oder *Grafana Enterprise* zurückgreifen. Dies widerspricht dem Prinzip *Secure by Default*, welches besagt, dass ein System von Anfang an so konfiguriert sein sollte, dass es die sichersten Konfigurationen nutzt, ohne dass der Benutzer zusätzliche Maßnahmen ergreifen oder zusätzliche Kosten tragen muss. Dies ist besonders für kleinere Unternehmen oder Universitäten mit begrenztem Budget wichtig, bei der Auswahl einer geeigneten Datenvisualisierungssoftware zu beachten. In Tabelle 1 ist die Verfügbarkeit von Security-Funktionen in den einzelnen Grafana Tarifen abgebildet. *Grafana Cloud* ist ein Freemium-Modell, bei dem das Hosting durch Grafana Labs übernommen wird. Gewisse Nutzerzahlen und Nutzungslimits sind kostenlos, danach muss

der Nutzer jedoch zahlen. Bei Grafana Enterprise steht es dem Nutzer offen, ob er die Instanz selbst hostet oder in der Cloud betreibt. Es existieren keine öffentlich zugänglichen Informationen über die Kosten von *Grafana Enterprise*. Glaubt man Nutzerberichten im Internet, bewegen sich die jährlichen Kosten auf rund 40.000$ [17].
Im Folgenden soll evaluiert werden, welche Sicherheitsfunktionen essenziell sind, besonders im Hinblick auf die Verwendung mit verteilten Systemen. *Grafana Open Source* bietet nur grundlegende Sicherheitsfunktionen an, die für einfache Anwendungsgebiete mit wenigen Mitarbeitern ausreichen sollten. Die erweiterten Sicherheitsfunktionen von *Grafana Cloud* und *Grafana Enterprise* sind vor allem für Anwendungen mit vielen Nutzern sinnvoll.
Eine Ausnahme bildet jedoch die fehlende Möglichkeit, Berechtigungen für Datenquellen in der Open-Source-Version festzulegen. Jeder Nutzer mit Editorrechten kann somit auf alle Datenquellen zugreifen, was dem Sicherheitsprinzip *Least Privilege* widerspricht. Dies ist besonders bei vielen verteilten Datenquellen kritisch, das die Nutzung der Open-Source-Variante anfälliger für Angriffe macht.
Ein ~~weiteres~~ wesentliches Element der Sicherheit ist die Datenbankverschlüsselung, wobei das regelmäßige Rotieren der Schlüssel meist ausreichend ist. Bei vielen eingebundenen, verteilten Datenquellen sind mehr Systeme potenziell gefährdet, sodass es sich lohnen kann, einen *Key Management Service (KMS)* zu verwenden, um eine erhöhte Sicherheit zu gewährleisten.
Das Auditing ist ein weiterer kritischer Aspekt, der in der Open-Source-Version nicht vorhanden ist. Bei einem Sicherheitsvorfall können die Aktionen keinem Nutzeraccount zugeordnet werden, was gegen die grundlegenden Sicherheitsprinzipien *Non-repudiation* (Nichtabstreitbarkeit) und *Accountability* (Verantwortlichkeit) verstößt.
Bei selbst gehosteten Grafana-Umgebungen, wie *Grafana Open Source* bzw. *Grafana Enterprise*, sollten regelmäßig Backups durchgeführt werden. Bei *Grafana Cloud* erfolgen die Backups automatisch.
Zusammenfassend lässt sich sagen, dass die fehlenden Berechtigungen für Datenquellen sowie das fehlende Auditing in *Grafana Open Source* kritisch zu betrachten sind. Nutzer sollten daher *Grafana Cloud* bzw. *Grafana Enterprise* verwenden.

| Funktion | Open Source | Cloud | Enterprise |
|---|---|---|---|
| SAML | × | ✓ | ✓ |
| LDAP | ✓ | ✓ | ✓ |
| Role-based access control | × | ✓ | ✓ |
| Data source permissions | × | ✓ | ✓ |
| Ordner/Dashboard permissions | ✓ | ✓ | ✓ |
| Datenbank Verschlüsselung | ✓ | ✓ | ✓ |
| KMS Integration | × | × | ✓ |
| Auditing | × | ✓ | ✓ |
| Secret Scanning | ✓ | × | ×/✓ |
| Request Security | × | ✓ | ✓ |
| Automatische Backups | × | ✓ | ×/✓ |
| Manuelle Backups | ✓ | × | ×/✓ |
| Sichere Konfiguration | ✓ | ✓ | ✓ |

Tabelle 1: Vergleich der Verfügbarkeit von einzelnen Security-Funktionen in Grafana Open Source, Grafana Cloud und Grafana Enterprise. [1]

# 5 Schluss

In dieser Arbeit wurde die Bedeutung von Sicherheitsmaßnahmen in Grafana, insbesondere im Kontext verteilter Systeme untersucht. Es wurde gezeigt, dass die Open-Source-Version von Grafana grundlegende Sicherheitsfunktionen bietet, die jedoch für den Einsatz mit verteilten Systeme oft nicht ausreichen. Die zusätzlichen Sicherheitsfunktionen in den kommerziellen Varianten Grafana Cloud und Grafana Enterprise erhöhen die Sicherheit signifikant. Insbesondere die Möglichkeit, Berechtigungen für Datenquellen festzulegen und umfassende Audit-Logs zu führen, sind entscheidende Vorteile. Dennoch sollte beachtet werden, dass der Einsatz der kommerziellen Varianten mit zusätzlichen Kosten verbunden ist, was insbesondere für kleinere Unternehmen und Bildungseinrichtungen eine Herausforderung darstellen kann. Insgesamt lässt sich feststellen, dass Grafana Cloud und Grafana Enterprise für Anwendungen in verteilten Systemen empfohlen werden, um eine angemessene Sicherheit zu gewährleisten. Weitere Arbeiten könnten sich mit dem Vergleich der Sicherheit zwischen verschiedenen Datenvisualisierungs-Tools beschäftigen, um die Auswahl einer Datenvisualisierungssoftware für Nutzer weiter zu vereinfachen.

# Literatur


[1] Grafana Labs. *Grafana*. 2024. URL: https://grafana.com (besucht am 11. 06. 2024).

[2] Grafana Labs. *Grafana Playground*. 2024. URL: https://play.grafana.org (besucht am 11. 06. 2024).

[3] Michael Nieles, Kelley Dempsey und Victoria Yan Pillitteri. *An introduction to information security*. Juni 2017. DOI: 10.6028/nist.sp.800-12r1. URL: http://dx.doi.org/10.6028/NIST.SP.800-12r1.

[4] ISO. *ISO/IEC 27001:2022*. URL: https://www.iso.org/standard/27001 (besucht am 16. 06. 2024).

[5] Grafana Labs. *CVE Database*. URL: https://grafana.com/security/security-advisories/ (besucht am 16. 06. 2024).

[6] Grafana Labs. *Grafana IAM*. 2024. URL: https://grafana.com/docs/grafana/latest/setup-grafana/configure-security/planning-iam-strategy/ (besucht am 11. 06. 2024).

[7] Grafana Labs. *Grafana RBAC*. 2024. URL: https://grafana.com/docs/grafana/latest/administration/roles-and-permissions/access-control/ (besucht am 11. 06. 2024).

[8] Grafana Labs. *Grafana Roles und Permissions*. 2024. URL: https://grafana.com/docs/grafana/latest/administration/roles-and-permissions/ (besucht am 11. 06. 2024).

[9] Grafana Labs. *Grafana Data source management*. 2024. URL: https://grafana.com/docs/grafana/latest/administration/data-source-management/ (besucht am 11. 06. 2024).

[10] Grafana Labs. *Grafana Encryption*. 2024. URL: https://grafana.com/docs/grafana/latest/setup-grafana/configure-security/configure-database-encryption/ (besucht am 11. 06. 2024).

[11] Grafana Labs. *Grafana Auditing*. 2024. URL: https://grafana.com/docs/grafana/latest/setup-grafana/configure-security/audit-grafana/ (besucht am 11. 06. 2024).

[12] Grafana Labs. *Grafana Secret scanning*. 2024. URL: https://grafana.com/docs/grafana/latest/setup-grafana/configure-security/secret-scan/ (besucht am 11. 06. 2024).

[13] Grafana Labs. *Grafana Request security*. 2024. URL: https://grafana.com/docs/grafana/latest/setup-grafana/configure-security/configure-request-security/ (besucht am 11. 06. 2024).

[14] Grafana Labs. *Grafana Backup*. 2024. URL: https://grafana.com/docs/grafana/latest/administration/back-up-grafana/ (besucht am 11. 06. 2024).

[15] Grafana Labs. *Grafana Upgrade*. 2024. URL: https://grafana.com/docs/grafana/latest/upgrade-guide/ (besucht am 11. 06. 2024).

[16] Grafana Labs. *Grafana Security hardening*. 2024. URL: https://grafana.com/docs/grafana/latest/setup-grafana/configure-security/configure-security-hardening/ (besucht am 11. 06. 2024).

[17] Reddit r/grafana. *Nutzerberichte über Kosten von Grafana Enterprise*. 2024. URL: https://www.reddit.com/r/grafana/comments/pb51dp/grafana_enterprise_cost_on_premise/ (besucht am 11. 06. 2024).

# Eidesstattliche Erklärung

Ich versichere, dass ich die vorliegende Arbeit ohne fremde Hilfe und ohne Benutzung anderer als der angegebenen Quellen angefertigt habe, und dass die Arbeit in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegen hat.

Alle Ausführungen der Arbeit, die wörtlich oder sinngemäß übernommen wurden, sind als solche gekennzeichnet.

Bei der Erstellung dieses Dokuments wurde künstliche Intelligenz (KI)-basierte Software ausschließlich zur sprachlichen Verbesserung und Korrektur verwendet.

Augsburg, 16. Juni 2024

(-)